UIC John Marshall Journal of Information Technology & Privacy Law

Volume 19
Issue 2 *Journal of Computer & Information Law - Winter 2001*

Article 2

Winter 2001

Data Mines and Battlefields: Looking at Financial Aggregators to Understand the Legal Boundaries and Ownership Rights in the Use of Personal Data, 19 J. Marshall J. Computer & Info. L. 313 (2001)

Julia Alpert Gladstone

DATA MINES AND BATTLEFIELDS: LOOKING AT FINANCIAL AGGREGATORS TO UNDERSTAND THE LEGAL BOUNDARIES AND OWNERSHIP RIGHTS IN THE USE OF PERSONAL DATA

by JULIA ALPERT GLADSTONE†

INTRODUCTION

The legal and business issues that surround financial aggregation services conducted on the Internet ("financial Web aggregation") do not garner attention because of customer interest in the service,[1] rather the interest in financial Web aggregation reflects the global hysteria[2] with the use of customer databases. Data mining and customer profiling have evolved with technology advancements during the past twenty-five years.[3] The ability of the Internet to collect greater quantities of data and to connect diverse data have created more sophisticated databases and has forced businesses to focus more intently on customer relationships, which has made customer information a valuable asset.

---

† Julia Alpert Gladstone is a professor of legal studies at Bryant College in Smithfield, Rhode Island. She researches the relationship of technology and the law particularly as it is unveiled in the Internet context. She writes on a broad range of legal developments in cyberspace, and Ms. Gladstone has been asked to speak at national and international conferences on timely Internet topics.

1. *See* Michele Heller, *Aggregators Playing by the Rules Get Nod in Poll*, Am. Banker 4 (Aug. 17, 2000) (reporting results from a Star Systems survey of computer users and Web aggregation services).

2. There is abundant literature on the conflict between the economic efficiencies which technology can produce by allowing greater insight into consumer preferences and the inherent loss of privacy. Computers, Freedom & Privacy is a conference, which has been held annually since 1991 where these issues are debated. *See generally* Computers, Freedom & Privacy 2000 <http://www.cfp2000.org> (accessed Nov. 26, 2000).

3. *See generally* Jane Kaufman Winn & James R. Wrathall, *Who Owns the Customer?: The Emerging Law of Commercial Transactions in Electronic Business Data*, 56 Bus. Law. 213 (Nov. 2000).

Financial Web aggregators gather a customer's data and then organize it on a single Web site that is then displayed to the customer for a fee. There is uncertainty and competition between parties claiming ownership in the same data.[4] Additionally, the privacy rights of the individuals from whom the information has been collected is also at stake.

This article begins by explaining the financial Web aggregation service that has often been referred to as "screen scraping" or "data aggregating" which was first developed by non-bank Internet portal companies as an opportunity to keep "eyeball contact" with the consumer.[5] There is no final version of the financial Web aggregation model because the service is augmented continually as the technology advances.

This article continues with a brief outline of the technology that facilitates financial Web aggregation before examining the two major federal statutes that will most influence the development of the financial aggregation service industry, namely the *Electronic Fund Transfer Act* ("EFTA")[6] and the *Gramm-Leach-Bliley Act* ("GLBA").[7]

Financial Web aggregation is still in its infancy; therefore, the rationales for applying these laws are sill being interpreted not only by the

---

4. *See* John Hackett, *Domesticating Account Aggregators*, 13:10 Bank Tech. News 1 (Oct. 2000) (discussing *First Union Corp. v Secure Com. Serv., Inc.*, No. 99-cv-519 (W.D.N.C. filed Dec. 30, 1999), a case subsequently dropped, and stating that one of nine claims made by First Union in its complaint against SCS was misappropriation of intangible trade values and commercial property by extracting time sensitive data and republishing it).

5. *See generally* David Hallerman, *All Data, All the Time: Aggregation of Consumer Financial Information by Third-Party Companies Threatens Banks But Opens Doors to E-Commerce*, 13:3 Bank Tech. News 1 (Mar. 2000) (discussing that portals have been the major players in consolidating Web data); *see generally* Miriam Leuchtet, *Aggregation Aggravation: Bankers' Recommendation on "Screen Scraping" – A Practice That Until Recently Horrified Them – Are Expected This Month from BITS*, 13:11 Bank Tech. News 58 (Nov. 2000) (explaining how banks once were furious over the practice of "screen scraping," yet since June 2000, all of the nation's largest banks have announced or are striking deals to offer aggregation services).

6. *Electronic Fund Transfers Act*, 15 U.S.C. § 1693 (2000). Previously known as the *Financial Institutions Regulatory and Interest Rate Control Act of 1978*, Pub. L. No. 95-630, § 2001, 92 Stat. 3728 (1978), it was passed to address the rapidly increasing volume of transactions involving electronic fund transfers. *Id.* Designated as Title IX of the *Consumer Protection Act* and now officially known as the *Electronic Fund Transfer Act*, its primary objective is to provide individual consumer rights for those participating in electronic fund transfers. *Id.* To implement EFTA, the Board of Governors of the Federal Reserve System is authorized to prescribe regulations. *Electronic Fund Transfers Act (Regulation E)*, 12 C.F.R. pt. 205 (2001).

7. *Gramm-Leach-Bliley Act*, Pub. L. No. 106-102, §§ 501–27, 113 Stat. 1338 (1999) (setting out procedures that financial institutions must follow in order to protect consumer privacy). GLBA has been codified at 15 U.S.C. § 6801 (2000).

courts but also by the implementing agencies.[8] Several common law theories are developing creatively as applied in the Internet context which may shed light on the allocation of risk and liability between the parties in a financial Web aggregation relationship; these theories are explained in Part III. The privacy and security interests of the consumers of financial Web aggregation services, which might have otherwise gotten compromised had large financial institutions not been involved, have received the necessary attention to assure protection.[9] This article concludes to suggest that attention which has been given to personal data privacy issues in the financial Web aggregation context ought to be broadened to general data gathering on the Internet.

PART I

Financial Web aggregation is a service that allows the customer to view all data from various accounts including financial institutions, stockbrokers, airline frequent flyer and other reward programs. The concept of accumulating and consolidating data for easy reviewing is not new or revolutionary. In fact, it was a feature banks provided for wealthy clients during the 1980s.[10] In a time when this information is available to the customer via the Internet with the use of a password and user name, the potential to consolidate and manipulate the information has significant new applications. Financial aggregation on the Internet gives the consumer the convenience of replacing numerous personal, identification number ("PIN")[11] protected sites with one master PIN to access the aggregator site. The time to log in to several sites is eliminated as well as the need to remember the numerous passwords. In addition, the single site offers the customer greater opportunity to analyze and manipulate his portfolio.

The major advantage to the aggregator is the additional contact with the customer, which is a marketing opportunity referred to as "sticki-

8. *See generally* Thomas P. Vartanian & Robert H. Ledig, *Scrape It, Scrub It and Show It: The Battle Over Data Aggregation* <http://www.ffhsj.com/bancmail/bmarts/aba_art.htm> (accessed Nov. 26,2000) (discussing a request issued on June 22,2000, by the Board of Governors of the Federal Reserve System for comment on aggregation issues).

9. The Banking Industry Technology Secretariat ("BITS"), the technology group of the Financial Services Roundtable (a Washington-based industry group), has formed a task force of fifteen financial institutions to develop business policies, practices and guidelines for aggregators to follow to reduce the risks of the practice. *See generally* The Fin. Serv. Roundtable, *BITS* <http://www.fsround.org/bitshome.html#FSRlogo> (accessed Nov. 26, 2000).

10. *See generally* Hallerman, *supra* n. 5.

11. PIN is literally the acronym for "personal identification number," but it is a term that is often used more loosely to refer collectively to the user names and passwords that allow access to Web sites or accounts that are "password protected" because they contain personal information. Vartanian & Ledig, *supra* n. 8, at ¶ 1.

ness" or "eyeball contact."[12] Another advantage to the aggregator is getting to know the competitors with whom the customer does business. Although the history of the financial Web aggregation business is short, it is evident that banks have not been the major players in this arena.[13] The recent initiative by the banks to become more important players in the financial Web aggregation market is viewed as critical to establishing customer relationships. The aggregator-customer relationship has been compared to the bank checking account-customer relationship, which is a fundamental relationship upon which more sophisticated business inevitably develops.[14]

Initially, the large aggregation companies were focused on providing aggregation services independently.[15] Now, at the close of the year 2000, we see that they have shifted their focus to being the technology providers for large financial institutions that want to offer this service.[16] Major banks that have the established role of trusted advisor are simply tapping the technology aggregator companies to offer aggregation services themselves.[17]

Financial Web aggregation services may be offered on a stand-alone basis but the trend is to offer them in conjunction with other financial services, most commonly bill payment.[18] The legal issues discussed in the remainder of this article refer to an augmented model of financial aggregation whereby the aggregator performs some electronic funds transfers. Upon contracting with an aggregator for services, the customer reveals all the names and identifying information of all accounts he wishes to have consolidated by the aggregator. The aggregator then goes to those sites with the requisite information, namely the customer user name and password to call up the data on the "provider information" site.[19] Permission to enter the provider information site is readily granted to the aggregator despite the fact that the true owner of the

12. Susan A. Funke, *"Content Is King:" Channeling Content to Public Web Sites: Industry Trend or Event*, 9:8 Searcher 66 (Oct. 1, 2000).

13. *See generally* Hackett, *supra* n. 4; *see also* Vartanian & Ledig, *supra* n. 8 (providing a brief history of data aggregation).

14. Telephone interview with John Jin Lee, Wells Fargo Bank Vice Pres. & Asst. Gen. Counsel (Nov. 16, 2000).

15. *See generally* Hackett, *supra* n. 4.

16. *See generally id.*

17. *See generally id.*

18. Paytrust.com was one of the first aggregator service providers that also allowed its customers to pay their bills electronically. Paytrust, *Paytrust Home, Corporate Vision* ¶ 2 <http://www.paytrust.com/htmlu/index.asp> (accessed Feb 4, 2000).

19. The focus in this article is on the aggregation services that are performed on financial services companies but aggregation firms can gather a variety of content or applications, therefore there is an occasional reference to information provider sites rather than just financial institution provider sites.

password is not accessing the site. This practice is what has led to the pejorative terms "screen scraping," "Web harvesting" or "secure data mining." HyperText Markup Language ("HTML") technology[20] is used to obtain the account information. Although this practice is most often done without the permission of the provider information site, HTML technology information gathering may also be conducted under an agreement between the parties.

There are limitations when connecting via HTML regardless of permissions granted. In particular, this process requires the aggregator to periodically log into the user account, extract account balances and hold this information on their own (the aggregator's) server for future presentation when the customer chooses to access the account. Consequently, this information is not "real time" and can only be as valuable as the aggregator's dedication to updating. Under the HTML model, in order for the customer to execute transactions he must enter the aggregator's site and then take a second step to link to the financial institution site and then take a third step which requires inputting his password to get to his individual secure account.

The alternative to the HTML connection is direct feed aggregation, which can only be accomplished by an agreement between the financial institution and the aggregator and requires the implementation of specific software. If the aggregator obtains the information from a financial institution using Open Financial Exchange ("OFX")[21] software, the customer can go to the aggregator Web site to receive real time, around-the-clock account information for all accounts.[22] In addition, once access into the aggregator's site is made the user can go directly to its account at the provider institution's Web site by clicking on a link within the aggregator's site. This avoids having to input an additional PIN or access code. In order for financial aggregation to become mainstream, agreements between the aggregator and the information provider will need to be negotiated which will also protect the customer's interests and provide a more robust service to the customer.[23]

---

20. HyperText Markup Language ("HTML") is the computer language that connects the World Wide Web. Rawdon Messenger, *A—Z of Cyberspace*, Evening Standard 26 (May 21, 2001).

21. *See generally* Open Fin. Exch., *Open Financial Exchange Home, About OFX* <http://www.ofx.net/ofx/ab_main.asp> (accessed Nov. 26, 2000) (explaining that Open Financial Exchange is used for electronic exchange of financial data).

22. *See generally* Open Fin. Exch., *Open Financial Exchange Home, About OFX, FAQs, How Does Open Financial Exchange Work?* <http://www.ofx.net/ofx/ab_faq.asp> (accessed Feb. 4, 2001).

23. Vartanian & Ledig, *supra* n. 8, at subpt. 4.1 (reviewing the steps First Union Corp. has instituted to manage the perceived risks).

The success of financial Web aggregators depends upon the full implementation of software that enables the aggregators and the financial or information-provider institution to share information easily. Currently, the software that is best suited to enable this sharing of banking data is OFX, a protocol that was developed by a loosely organized consortium consisting of CheckFree, Intuit and Microsoft.[24] The development and widespread adoption of this protocol is fascinating and characteristic of the Silicon Valley entrepreneurship that has driven the Internet revolution.[25] The attractive screens that are displayed on a computer to deliver information from various networks throughout the world that we refer to as the Internet are the result of electronic impulses and software technology. There are different grades or levels of electronic documenting software that range from basic syntax which provides the instruction for the very formation of an electronic document to language or grammar, which includes the words describing the purpose for the instruction of the syntax.[26] One cannot have a grammar without an underlying syntax.

The most common computer grammar on the Internet today is HTML. It is HTML that creates the graphics and the "hot" links that connect the Web and enable browsing.[27] HTML is based upon a syntax called Standard Generalized Markup Language ("SGML").[28] SGML was the original technical standard that encoded data to create electronic documents. There are three types of information that can be captured by electronic document formats and three classes of formats.[29] In very simplified terms, the types of information that can be captured are: (1) formatting, which is how the text looks to the reader including bold lettering, italics or underline, (2) logical structure, such as chapters, head-

24. *See generally* Open Fin. Exch., *supra* n. 22. Check free, Intuit and Microsoft have been collaborating since 1993 but have not publicly announced a formal relationship. Steven Marlin, *Integrion Wraps Up Operations: Banks to Manage Middleware: Company Operations*, 5:37 Bank Systems + Technology 12 (May 1, 2000).

25. The Interactive Financial Exchange ("IFX") is a standard that is being built on the experience of OFX and Integrion GOLD specifications that seeks to serve online financial services as well. Robin Cover, *The XML Cover Pages, The XML Cover Pages Home, Site Index, Interactive Financial eXchange (IFX)* ¶ 12 <http://www.oasis-open.org/cover/ifx.html> (last updated Nov. 29, 2000).

26. *See generally* Winchel "Todd" Vincent, III, *XML and the Legal Foundations for Electronic Commerce: Legal XML and Standards for ythe Legal Industry*, 53 SMU L. Rev. 1395 (Fall 2000) (providing a thorough explanation of the characteristics and varieties of electronic document formats).

27. Julia Gladstone, *Using the Internet for Effective Legal Research* 29, 33 (PLI Pat., Copy., Trademarks, & Literary Prop. Course Handbook Series No. G0-0019, 1998).

28. *See generally Standard Generalized Markup Language* <http://whatis.techtarget.com/WhatIs_Definition_Page/0,4152,214201,00.html> (accessed Nov. 26, 2000). This standard was promulgated by the International Organization for Standards. *Id.*

29. Vincent, *supra* n. 26, at 1398–99.

ings, paragraphs or subparagraphs and (3) data, which are pieces of information by which the document can be sorted or indexed.[30] The three document formats are (1) page description, (2) mark-up-based and (3) compound document.[31]

HTML is a document mark-up-based language/grammar whereby the logical structure and the data are captured by tags.[32] HTML language is described as being based on an element that is the combination of a beginning tag and an end tag and everything in between.[33] An example of an HTML element is: <FONT Color ='Green'>Spot sees the bone.</FONT>.

OFX is a grammar that was developed to address the specific needs of the financial services and banking industry. OFX supports transactional Web sites by streamlining the process financial institutions need to connect multiple customer interfaces, processors and systems integrators. When broken down, one finds that OFX is a document format with customized tags or elements and although it may look like HTML, it is not constrained by a predefined set of tags. OFX frees the format from the logical structure that thus separates OFX from the SGML syntax. In creating a grammar software to directly address the needs of its clients, the OFX consortium in fact developed a refined syntax.

The problems with HTML, namely that the tags are predefined thus making it a "dumb" document format,[34] are being addressed independently by software developers. Beginning in 1997, the World Wide Web Consortium ("W3C") supported an effort to develop the eXtensible Markup Language ("XML") which is based on the very idea of freeing elements from the HTML standard to create data that can be retrieved more easily.

XML is a powerful and useful tool in business because it allows raw data to be turned into useful information without human intervention. The XML standard is based on "document type definition," which is a set of rules that define the type, number and order of elements that can appear in an XML document.[35] XML is not industry specific, rather it is a syntax that allows software to identify and capture pieces of information from a document automatically. Many industries have already adapted

30. *Id.*

31. *Id.* at 1399.

32. *Id.*

33. *Id.*

34. Winchel "Todd" Vincent, III, *XML and the Legal Foundations for Electronic Commerce: Legal XML and Standards for the Legal Industry*, 53 SMU L. Rev. 1395, 1400 (Fall 2000).

35. *Id.* at 1401.

XML taxonomies to serve their purposes.[36] OFX, however, was developed independently of XML.

PART II

Financial Web aggregation appears to the consumer like a service that ought to be governed by banking regulators. In fact, just over half of the respondents to a Star Survey assumed that aggregators were required to follow banking rules, while 92 percent said that they should be so regulated.[37] EFTA and *Regulation E*,[38] which were enacted by Congress in 1978 as part of the *Financial Institutions Regulatory and Interest Rate Control Act of 1978*,[39] were specifically designed to protect consumers in retail electronic-fund transfer systems.

The EFTA originated when the primary vehicles for electronic fund transfers were automated teller machines ("ATM") and point of sale ("POS") terminals, telephone payment systems and automated clearinghouse transactions.[40] Therefore there has been some difficulty in applying *Regulation E* to financial Web aggregation.

An electronic fund transfer ("EFT") must have three components in order to be subject to *Regulation E*. There must be: (1) a transfer of funds, (2) that is initiated by electronic means, and (3) that either debits or credits a consumer account held directly or indirectly by a financial institution.[41] There is little debate that activity in an aggregation account will result in funds being transferred electronically to either debit or credit a consumer account.[42] It is also quite clear that a financial aggregator is at a minimum indirectly holding said account.

The reason why it is unclear whether *Regulation E* applies to financial Web aggregators is due to the uncertainty surrounding the definition of financial institution.[43] The Board of Governors of the Federal Reserve System has requested comments on aggregation issues with specific attention to the question whether an aggregator ought to be defined as a financial institution under *Regulation E* in connection with a proposed

36. *See e.g. A Vast Unchartered Cave*, 5:1 Bryant Bus. 9 (Winter 2001) (stating that protocols have been developed by advertising ("ADXML") human resources ("HRXML"), printing ("Printml") and marine trading ("MTML")).

37. Heller, *supra* n. 1, at 4.

38. 12 C.F.R. 205.

39. 15 U.S.C. § 1693.

40. *See generally* Thomas P. Vartanian, Robert H. Ledig, & Lynn Bruneau, *21st Century: Money, Banking & Commerce* <http://www.ffhsj.com/21stbook/> (accessed Jan. 11, 2001).

41. 12 C.F.R. at pt. 205.3(b).

42. *See generally* Hackett, *supra* n. 4.

43. *See generally Id.*

revision to *Regulation E* issued on June 22, 2000.[44] Comments were due by August 30, 2000, but it remains uncertain whether the Federal Reserve Board will choose to clarify this particular matter.[45]

A "financial institution" is defined under *Regulation E* to include "a bank, savings association, credit union, or any other person that directly or indirectly holds an account belonging to a consumer, or that issues an access device and agrees with a consumer to provide electronic fund transfer services."[46] An "[a]ccess device means a card, code or other means of access to a consumer's account."[47] Therefore, there may be multiple financial institutions in a single EFT transaction.[48]

The following are two scenarios that present financial Web aggregation activities meriting the protection provided by *Regulation E*. In scenario #1: Customer A accesses his aggregation account with his aggregator PIN to review his account. He intends to transfer $1,000 from his bank account to purchase ten shares of stock at his brokerage account. He executes this transaction by clicking the bank icon within the aggregation site. This takes him directly to his secure page on the bank site where he authorizes the withdrawal of funds and a subsequent purchase at the brokerage site. Once again, this is possible because the aggregator has entered into agreements with the bank and broker and shares proprietary software with both information providers.

In scenario #2, Customer B is at his personal secure page at his bank site where he clicks on the aggregator icon to go directly, i.e. without any additional PINs, to his brokerage account where he buys the ten shares of stock. Once again, he only needs to log in once for the complete service.

Regulation E has six major substantive requirements[49] that offer consumers protection in EFT transactions; the relative importance of these to the financial Web aggregation services is explained below. The above scenarios demonstrate the need for a *Regulation E* requirement that establishes error resolution procedures[50] to be applied to financial Web aggregators.

Suppose a computational error is made by the aggregator, whereby $10,000 rather than the intended $1,000 was withdrawn from the bank, and yet only ten shares were then purchased. *Regulation E* requires that

44. Vartanain & Ledig, *supra* n. 8, at subpt. 5.1.3.

45. *See* Hackett, *supra* n. 4, at ¶ 34 (recounting a remark by Kyung Cho-Miller, a lawyer at the Federal Reserve, that "the Federal Reserve now will consider the comments and 'take appropriate action' by the end of the year.").

46. 12 C.F.R. at pt. 205.2(i).

47. 12 C.F.R. at pt. 205.2(a)(1).

48. Vartanian, Ledig & Bruneau, *supra* n. 39, at 67.

49. 12 C.F.R. at pts. 205.4–205.9, 205.11.

50. 12 C.F.R. at pt. 205.11.

the financial institution must investigate and determine whether an error has occurred within ten days of receiving notice; and if the investigation takes longer, the institution must recredit the consumer's account in the amount of the alleged error within ten business days. If the aggregator is not covered by *Regulation E,* it is unclear whether the bank is required to bear the burden of the error, in particular because the customer may have never directly accessed the account in order to conduct the transaction.[51] Presently, banks are absorbing any costs to avoid customer dissatisfaction but they believe the definition of financial institution ought to be broadened.[52]

The application of *Regulation E*'s limitation on consumer liability for unauthorized EFTs in the financial Web aggregation context is also unclear. *Regulation E* limits consumer liability for unauthorized EFTs[53] to the lesser of $50 or the actual amount transferred prior to the time the customer notifies the financial institution, if the customer notifies the financial institution within two days of learning of theft or loss of the device.[54] If the customer fails to notify the institution in a timely manner the consumer's liability may not exceed $500.[55]

A financial Web aggregation consumer may argue that he never authorized a transaction that was processed by the aggregator using the PIN.[56] If the aggregator is not held liable, the bank will again need to compensate the customer unless an alternative agreement has been previously reached. Some financial institutions are putting responsibility on the customer by contract when an aggregator's services are engaged.[57]

The remaining four substantive requirements of *Regulation E* address disclosure and notice requirements. *Regulation E* prohibits a financial institution from issuing an access device unless the customer has requested the device orally or in writing,[58] and a readily understood written disclosure statement of the terms and conditions of the EFT service must be provided at the initial time of contracting or before the first

51. Arguably the bank is covered simply because it is a bank and therefore falls squarely within the definition of a financial institution under 12 C.F.R. at pt. 205.2(i).

52. "If it quacks like a duck and walks like a duck then it should be treated like a duck." Lee, *supra* n. 14.

53. Unauthorized transfers are defined as transfers "from a consumer's account initiated by a person other than the consumer without actual authority to initiate the transfer and from which the consumer receives no benefit." 12 C.F.R. at pt. 205.2(m).

54. 12 C.F.R. at pt. 205.6(2). However, it is not clear how this is section would apply to aggregators.

55. *Id.*

56. Vartanian & Ledig, *supra* n. 8, at subpart 5.1.2.

57. *Id.*

58. 12 C.F.R. at pt. 205.5(a)(1).

EFT is made.[59] Any changes in terms or conditions to the relationship must be mailed or delivered to the customer[60] and receipts of EFT transactions must be made available to the customer.[61] The consumer protections of *Regulation E* are particularly well suited to financial Web aggregation services.

Financial Web aggregation activity occurs in a gray area, and while protecting consumers is a prime consideration of regulators, there is concern with the ramifications of over-regulating. If the Federal Reserve Board were to decide to include non-bank aggregators within the definition of financial institution for purposes of *Regulation E*, that would also include other professionals offering similar services to their clients. For instance, CPAs, attorneys and stockbrokers often consolidate their clients' accounts, offer management services and may even execute transactions. Financial aggregators are acting as agents for their clients. How often are these same services provided under power of attorney contracts? Would a change in the definition of financial institution under *Regulation E* implicate these relationships as well? The automation of the aggregators data-feed software makes them stand apart from these other professional groups and arguably would justify the Federal Reserve's broadening of the definition of financial institution to include financial Web aggregators but not other professionals.

Several federal statutes have been enacted over the years that address the protection of consumer privacy in matters of personal finances.[62] In the area of financial Web aggregation, the customer himself is broadening the frontier of his privacy exposure. The GLBA[63] establishes new obligations and rights with respect to consumer privacy that regulatory agencies have promulgated regulations to enforce.[64] Once again, the relevant provisions are enforceable against a financial institution that is defined as "any institution the business of which is engaging in financial activities as described by section 4(k) of the Bank Holding Company Act."[65] Unlike the situation under *Regulation E* under the

59. 12 C.F.R. at pts. 205.4(a), 205.7(a).

60. 12 C.F.R. at pt. 205.8(a)(1).

61. 12 C.F.R. at pt. 205.9(a).

62. *See e.g. Right to Financial Privacy Act*, 12 U.S.C. §§ 3401–22 (2000) (prohibiting unauthorized access to and sharing of an individual's financial data by federal agencies); *Fair Credit Reporting Act*, 15 U.S.C. § 1681 (2000) (restricting access to individual's credit information).

63. 15 U.S.C. §§ 6801, *et seq.*

64. The Office of the Comptroller, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, and the Office of Thrift Supervision jointly issued final privacy rules implementing the GLBA, 12 C.F.R. at pt. 40, 12 C.F.R. at pt. 216, 12 C.F.R. at pt. 332 and 12 C.F.R at pt. 573, respectively. The Federal Trade Commission issued its own separate privacy rules at 16 C.F.R. at pt. 313.

65. 113 Stat. at 509(3)(A).

GLBA there is certainty that financial Web aggregators are included within the definition of financial institution. In the explanation which precedes the final rules issued by the Federal Trade Commission implementing the GLBA, the definition of a financial institution includes "an Internet company that compiles, or aggregates, an individual's on-line accounts (such as credit cards, mortgages, and loans) at that company's [W]eb site as a service to the individual, who then may access all of its account information through that Internet site."[66]

In general, the GLBA: (1) requires disclosure of policies and practices regarding disclosure of private financial information, (2) prohibits disclosure of private financial information to unaffiliated third parties unless consumers are provided a right to opt out; and (3) requires the establishment of safeguards to protect the security and integrity of private financial information.[67] The privacy protections apply to "nonpublic personal information," which means personally identifiable financial information provided by a consumer to a financial institution or resulting from any transaction or any service performed for the consumer or otherwise obtained by the financial institution. The restriction on the use of personally identifiable information suggests that disclosure about individuals cannot be made if the identity of the customer is also made available.

Before a financial institution can share personal information with nonaffiliated parties, the institution must disclose the practice to the consumer and give him an opportunity to opt out.[68] The opt out option must be well explained. It is noteworthy that the GLBA adopted an opt out approach rather than requiring the consumer to consent prior to the sharing of his information with nonaffiliated third parties. The GLBA therefore defaults in favor of the institution revealing consumer information. In addition, there are several exceptions whereby institutions may share consumer's personal information with third parties without giving the consumer the opportunity to opt out.[69]

There is considerable debate among privacy experts whether the privacy provisions of the GLBA or any legislation are sufficient to protect an individual's privacy interest,[70] a discussion which extends beyond this article the purpose of which is to explore the applicability of existing United States laws to financial Web aggregation services.

---

66. 65 Fed. Reg. 33655 (May 24, 2000).

67. 15 U.S.C. § 6802.

68. 15 U.S.C. § 6802(b)(1)(A)–(C).

69. 15 U.S.C. § 6802(b)(2).

70. *See generally* Karl D. Belgum, *Who Leads at Half Time?: Three Conflicting Visions of Internet Privacy*, 6 Rich. J. L. & Tech. 1 (1999) (discussing the problems with applying existing privacy laws to the online market).

The GLBA covers the activities of financial Web aggregators and requires full disclosure of an institution's privacy practices to the consumer on a regular basis. The substantive provisions of the GLBA are the most comprehensive privacy protections for private industry to be enacted in the United States to date.

PART III

The discussion of the statutes in the previous section illustrates the likelihood that if applied consistently, consumer interests in financial Web aggregation transactions would be protected. There still exists a contingent of information-provider sites that would like to stop the practice of financial Web aggregation. In Part III of this article, one statute and several common law causes of action that have been uniquely applied in the Internet context are explained as they apply to financial Web aggregating.

Congress enacted and has amended the *Computer Fraud and Abuse Act* ("CFAA")[71] to protect against unauthorized access to computers or access to a computer in excess of authorization. CFAA makes it a misdemeanor "to knowingly access a computer without authorization or in excess of authorization in order to obtain information contained in a financial record of a financial institution or in a consumer file."[72] Consequently, an aggregator who extracts information from an information provider without express consent from the customer could be liable under the CFAA. It does seem unlikely that such a circumstance would arise if the information is password protected and the password has been given by the customer to the aggregator. There is only the question of the extent of the authority that the customer can give the aggregator when he gives away his PIN to his account at the information provider's site. If the information site-owner can limit by contract the conditions and use of the PIN, then it is conceivable that the aggregator's use of the PIN could run afoul of the CFAA.[73] This again brings into focus the question of who is the real owner of this financial data.

The security risks that arise in financial Web aggregation are being addressed primarily through administrative and technological solutions. Encryption is built within the OFX protocol. The Secure Sockets Layer ("SSL") technology should minimize if not eliminate any hacking or other fraud.[74] Storing customers' passwords and identification numbers on

71. 18 U.S.C. § 1030 (2000).

72. *Id.*

73. *See Am. OnLine, Inc. v. LCGM, Inc.*, 46 F. Supp. 2d 444, 450 (E.D. Va. 1998) (suggesting that a breach of an online service's terms of use is an unauthorized use).

74. *See generally* Whatis?com, *Whatis?com Home, All Categories, Networking, Security, Secure Sockets Layer* <http://whatis.techtarget.com/WhatIs_Definition_Page/

different servers is another practice that improves security. Several financial institutions are setting up security guidelines for participating aggregators to follow.[75]

Several intellectual property rights of the information provider may be compromised by the aggregator's activities. The aggregator's Web site presents information from various other sites and it may also include the other corporation's logo which naturally suggests a relationship between the two entities. Although the consumer may not be confused while on the aggregator's site that he is at the information provider's site, which would be necessary to bring an action for trademark infringement,[76] the experience of the customer with the aggregator could rub off on the institution. Similarly, some false designation may be attributed to the aggregator from having the information provider's institution logo on the site. Some institutions have resolved this dilemma with a disclaimer of affiliation that is placed on the aggregator's site. Thus far, no Web aggregator infringement cases have reached the litigation stage.

Taking information from one Web site and reformulating on another involves copying which may be prohibited under copyright law.[77] A claim for copyright infringement is only plausible if the aggregator is appropriating the original expression of the "scraped site." In addition, factual information is not copyrightable. In most cases, aggregators will retrieve the factual information without its original expression and present it on its own Web site creatively, in which case there are no apparent copyright concerns.

The jurisprudence of intellectual property on the Internet is currently evolving, and an important case in the area is *Ticketmaster Corp. v. Tickets.Com, Inc.*[78] In that case, the trial judge denied Ticketmaster's ("TM") motion for a preliminary injunction to stop Tickets.Com from using computer software or "robots" to search or "crawl" TM's site for information about tickets, which it then used on its own site to attract viewers.[79] The judge gave serious consideration, however, to the theory that the very "crawling" constituted an infringement on copyright.[80] He described the electronic devices known as "Web crawlers" or "spiders."

0,4152,343029,00.html> (accessed Nov. 26, 2000) (providing an in-depth look at SSL technology).

75. *See generally* Vartanian & Ledig, *supra* n. 8.

76. *Id.* The *Lanham Act* has been amended by the *Federal Trademark Dilution Act of 1996*, 15 U.S.C. § 1125 (2000), which protects companies against "the lessening of the capacity of a famous mark to identify a good or service." *Id.*

77. *Copyright Act*, 15 U.S.C. § 1051 (2000).

78. 2000 U.S. Dist. LEXIS 12987 (C.D. Cal. Aug. 10, 2000).

79. *Id.* at **8–9; *see generally* Stephen T. Middlebrook & John Muller, *Thoughts on Bots: The Emerging Law of Electronic Agents*, 56:1 Business Lawyer 341 (Nov. 2000) (explaining "robots," or "bots," and "Web crawlers").

80. *Ticketmaster*, 2000 U.S. Dist. LEXIS 12987 at *11.

They "enter the TM computers electronically through the home page and make a note of the URL's (electronic addresses) of the interior Web pages. They then methodically extract the electronic information from the event page . . . and copy it temporarily (for 10-15 seconds) on its own computers."[81] The judge found that "the copying is transitory and temporary and is not used directly in competition with TM, but it is copying and it would violate the Copyright Act if not justified."[82] The judge also found that the Tickets.com copying was justified under the fair use doctrine.[83] Specifically, he analogized the actions of Tickets.com to reverse engineering.[84] Further judicial and legal scholarly attention to this theory suggests that the mere recording of information prior to transmitting it onto one's own site could itself constitute a copyright infringement.[85] Thus, the means by which Web aggregators obtain their information could be found to violate copyright laws. Once again, however, we must ask who owns the subject information.

In the same motion for a preliminary injunction, the judge considered but dismissed as not applicable a relatively unknown and seldom-used cause of action that has been recently revived to stop competitor Web sites from infringing upon each other's rights.[86] The theory of trespass to chattels is a common law action in tort that has recently been deemed applicable to cyberspace in that "electronic signals [are] sufficiently tangible to support a trespass cause of action."[87] The theory has received widespread attention and acceptance since the order granting preliminary injunction in favor of eBay in the Northern District of California.[88]

EBay is one of the biggest success stories on the Internet.[89] It is an online auction house that has "15.8 million registered users bidding on 62.5 million auctions each year."[90] The seller offers his product for a period of time to the highest bidder, and the sales transaction takes place solely between the two interested parties.[91] In addition to generating

81. *Id.* at **8–9.

82. *Id.* at *11.

83. *Id.* at *12.

84. *Id.* at **12–13.

85. Middlebrook & Muller, *supra*, n. 79, at 359.

86. *Ticketmaster*, 2000 U.S. Dist. LEXIS 12987 at **14–15.

87. *EBay, Inc. v. Bidder's Edge, Inc.*, 100 F. Supp. 2d 1058, 1069 (N.D. Cal 2000) (citing *Thrifty-Tel v. Bezenek*, 46 Cal. App. 4th 1559, 1566 (1996)).

88. *Ticketmaster*, 2000 U.S. Dist. LEXIS 12987 at *14.

89. Middlebrook & Muller, *supra* n. 79, at 359.

90. *Id.*

91. *EBay*, 100 F. Supp. 2d at 1060. While payment for goods can be made with a credit card, that does actually involve a third party. *Id.* However, a new type of service is evolving to assist those sellers that do not wish to process credit cards, but cannot facilitate cash payments; yet it is still unclear how they will be viewed for regulatory purposes. *Id.*

similar, yet smaller, competitor online auction houses, such as Yahoo! and Amazon.com, eBay has spawned a subindustry of metasearch sites which offer comparison shopping among various auction sites.[92] Thus, if a buyer is seeking a particular item he may enter a search request on a metasearch auction site that will scour all auction sites for available matching items.[93] Bidder's Edge (BE) is in the business of conducting such metasearches that included eBay.[94] EBay requested that BE stop searching its site claiming that these outside metasearch engines reduced the performance of eBay's Web site.[95] BE uses "an automatic or robotic computer script to periodically invade the eBay site (and presumably the sites of others) and make a verbatim copy of eBay's auction listing pages across numerous categories of items."[96] BE metasearches are conducted by computer programs or software robots. The judge ruled that the software robots "consume the processing and storage resources of a system, making that portion of the system's capacity unavailable to the system owner or other users. [Citation omitted.] Consumption of sufficient system resources . . . can overload the system such that it will malfunction or 'crash.'"[97] With this understanding of BE's actions, the court ordered a preliminary injunction based upon the theory of trespass to chattels.[98]

The theory of trespass to chattels is unlikely to apply to financial Web aggregators because very little interference with the financial institution or information provider's system is necessary to obtain the needed information. The district court in the eBay case focused not only on the actual harm caused by BE but the reduction in use of eBay's system that could potentially result from other noncomplying auction aggregators. The specificity of the searches by financial Web aggregators and the terms of agreement under which the searches are often now being conducted would make trespass to chattels claims untenable.

CONCLUSION

The issues and concerns presented by financial Web aggregation are the key issues that society must address as technology makes information dramatically cheaper to collect, store and display. The ease with

PayPal is the largest of these companies. *See generally* Jathon Sapsford, *PayPal Sees Torid Growth with Money-Sending Service* <http://www.paypal.com/html/wsj3.html> (accessed Nov. 26, 2000).

92. Middlebrook & Muller, *supra* n. 79, at 359.

93. *Id.* at 360.

94. *Id.*

95. *Id.*

96. *Id.* at 361.

97. *EBay*, 100 F. Supp. 2d at 1061.

98. *Id.* at 1072.

which we can manipulate data has changed the way commerce is conducted. The use of customer databases has become a critical strategy to successful business, and, thus, consumer profiles are a valuable intangible asset. The new generation of Web aggregators and data miners can offer a staggering array of content that is used in business. Often times property rights in the data are not recognized under intellectual property laws. The information that is gathered and displayed by financial Web aggregators belongs to the consumer. Although this is evident, it is a fundamental relationship that may need to be asserted in particular circumstances. The personal information belongs to the consumer, and the consumer has a fundamental right to privacy in this data that is best protected when it is treated as a property right.[99]

99. *See generally* Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. Pa. L. Rev. 707 (1987) (discussing the need for a neutral concept of privacy in light of modern technological advancements).